© THE QUEEN'S PRINTER FOR ONTARIO
1999

REPRODUCED WITH PERMISSION

L'IMPRIMEUR DE LA REINE POUR L'ONTARIO

REPRODUIT AVEC PERMISSION

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel: (416) 362-5211
Toll free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

Information
and Privacy
Commissioner/
Ontario

Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation

Ann Cavoukian, Ph.D.
Commissioner
September 1999

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

The Information and Privacy Commissioner gratefully acknowledges the work of John Eichmanis for his contribution in preparing this report.

Cette publication est également disponible en français.

This publication is also available on the IPC Web site. Upon request, this publication will be made available on audio tape to accommodate individuals with special needs.

100-05386/

Executive Summary

The paper begins with a brief overview of the concept of privacy. Having introduced the terms of reference, the paper delineates the traditional ethical and human rights approaches to the topic. Privacy, it is noted, is considered to be a fundamental human right — a moral and social "good," and is recognized as such in numerous international covenants and declarations. However, specific laws protecting privacy vary considerably and are often vague or limited in scope. Principally, there are two main approaches to protecting an individual's "right" of privacy: legislation and self-regulation, with the Europeans favouring the former and the Americans inclined towards the latter. It is argued that both legislation and self-regulation have a role to play in any discussion of privacy matters — neither should be dismissed outright when exploring privacy in the context of the private sector.

The paper then turns to examine privacy and the marketplace. A principle theme of this section is the vital importance of individual choice. Any discussion of "choice" must include an analysis of an individual's relative "bargaining power," or range of options available in various situations. When interacting with public sector (government) organizations, an individual is typically faced with a situation in which he or she has asymmetrical bargaining power (i.e., limited, if any, choice). The government is often the sole provider of a good or service and may in fact compel an individual to deal with it (e.g., to receive licences, permits or publicly conferred benefits). Conversely, the private sector usually offers an individual some range of choices and options — either from a single company or its competitors. Ultimately, customers can "vote with their feet," taking their business elsewhere if they do not wish to deal with a particular company or organization.

In reality, however, any one individual may not have the entire range of options of the whole marketplace available to him or her personally. Thus, in many instances, the individual may be faced with a situation in the private sector comparable to his or her dealings with the government. This limitation on personal choice, while very real, appears to be changing. Firstly, personal information is coming to resemble a commodity — a scarce good — that is highly desirable; consequently, it is gaining considerable value (somewhat like a medium of exchange). Secondly, as advanced technology permeates throughout our social and economic lives, an increasing range of options and alternatives will be available for receiving goods and services, as well as for setting the "terms" for one's interactions with vendors.

The well known adage, "knowledge is power," has perhaps never been more true. The paper further details the existing "market" as it relates to privacy, in terms of economic theory and the current unstructured nature of the market for personal data. An important issue highlighted here is the inappropriate secondary uses of personal information (the selling or exchanging of personal information to third parties without the knowledge or consent of the individual). Personal information has become a commodity that is being bought and sold by companies, almost entirely at the expense of personal privacy. This practice not only violates fair information practices (internationally recognized data protection principles), but also undermines consumer confidence and trust in business.

To counter this imbalance of power, a number of scholars (and emerging software companies offering the services of "infomediaries" or information intermediaries) have called for the development of a structured market for privacy. This market relies upon the recognition of personal information as property, with its ownership belonging to the individual to whom it relates.

Working with this assumption (a situation not yet addressed by law), a structured market for personal data could be established, similar to markets for other tangible and intangible goods. It is argued that recognizing an individual's property rights for the commercial uses of his or her personal information would be another means by which the increasing erosion of privacy could be stemmed. A marketplace for personal data would enable people to choose to consent to the uses of their personal information, in exchange for some benefit they valued. Conversely, permission could be withheld if the benefit was not considered to be sufficient to merit the degree of disclosure requested. While there is no consensus on how such a market would actually work, it is clear that a quasi-market is already emerging through the development of loyalty marketing cards (e.g., AirMiles Reward Miles cards and other loyalty programs).

Regardless of whether a structured market develops or whether individuals are recognized to hold a property right interest in their personal data, new technological means are being developed to assist individuals in protecting their own privacy. Privacy-Enhancing Technologies (PETs) are an emerging class of software covering a range of protective measures. These technologies typically incorporate one of the following mechanisms to protect an individual's privacy: strong encryption, anonymizing and/or pseudonomyzing programs, personal databanks, and various types of electronic payment systems. Other systems, based on international standards such as the Platform for Privacy Preferences (P3P), will automatically review a Web site's privacy policy and only permit a transfer of information that is consistent with a user's wishes. Similarly, Intelligent Software Agents (ISATs) are being developed to undertake a variety of tasks on behalf of individuals according to their predetermined instructions and restrictions. As noted earlier, infomediaries could employ ISATs to act as a buffer between a vendor and a purchaser, communicating only the amount of personal information required to complete a transaction.

As companies seek to improve their relationship with their customers and potential customers, many are implementing privacy protection policies, as well as industry-based privacy codes and privacy seals to govern the operation of their electronic businesses. The combination of improved data protection practices by businesses and enhancements in the power of encryption, anonymizing/ pseudonomyzing programs, infomediaries and other PETs, will go a long way towards protecting people's personal information. Over time, these developments will help to restore the balance of power between businesses and individuals regarding the uses of their personal information.

This paper recognizes that privacy will continue to be an important economic and social issue. The current state of privacy protection is insufficient, and, in the long run, untenable. New technologies are emerging to redress this imbalance, but it is unlikely that technology alone

will be sufficient. New types of relationships are emerging between individuals and businesses regarding the relative importance and value of customer information. A structured market for personal data is slowly emerging in various sectors. It is too early to tell whether this will lead to a formal recognition of what is presumed by most — an individual's ownership of personal data relating to himself or herself.

Legislated protections must continue to safeguard fundamental human rights relating to the state, with restrictions placed on the uses of one's personal information by government. The first element of any privacy architecture would include data protection as embodied in fair information practices and implemented through legislation in the context of the public sector. Protections extending to the private sector would come in the form of legislation or meaningful self-regulation. Any consideration of market-based protections would only be made in the private sector, in the context of commercial transactions. Information property rights would form an important element of market-based protections.

Regardless of how a new privacy architecture is designed or developed, one thing is clear — privacy has become a leading issue of concern to consumers, and in turn, to businesses and legislators. The formation of a structured market for personal data may appear at odds with the belief that privacy is a fundamental human right. However, one could also argue that such a market is a natural, evolutionary development; it is also a recognition of what is in fact occurring in the business world today. In the end, two key issues are of paramount importance for the development and operation of any market-based scheme: transparency and consumer choice. Individuals must be able to know what businesses are doing with their personal information and be able to grant or withhold their consent regarding the uses of their information. If a market for personal data helps to protect privacy and promotes freedom of choice, then we support it. If, however, the marketplace acts against the interests of individuals, then Privacy-Enhancing Technologies will grow even more important in helping individuals to protect their privacy. Much remains to be determined.

Abstract

The nature of privacy debate, virtually throughout the world, has been significantly recast over the last decade, coinciding with what could be termed as the "Internet decade." The prevailing technology-driven reality has, in large part, contributed to a shift in the public's perception of privacy matters. The forum of discussion has moved from revolving almost exclusively around public sector institutions, to one that now preoccupies organizations in the private sector. For much of the 1970s and 80s, the focus of privacy concern was on government's potential (and often actual) ability to engage in privacy-intrusive activities. The spotlight has now turned to cast a light on the role of private sector companies — the privacy implications of their activities and the growing commercial value of consumers' personal information.

Thus, no one should be surprised that in the wake of this altered privacy landscape, the articulation of privacy issues and their resolution has also shifted. The framework for discussing privacy issues now encompasses a private sector commercial perspective, in addition to the traditional human rights approach.

The aim of this paper is to explore these two different perspectives on privacy. A key question to be addressed is whether any insights gleaned from the economic rights approach could provide a viable set of policy prescriptions for addressing current and emerging privacy issues. Of particular interest is the outcome for individual control and choice, were a market framework for protecting privacy to be adopted. Can privacy issues be resolved by relying on the economic self-interest of individuals to make the appropriate decisions as to the degree of privacy they wish to maintain?

The perspective taken in this paper is as follows: to the extent to which these different approaches can strengthen an individual's capacity to control the flow of his or her personal information and his or her ability to make choices about the collection, use and disclosure of this information, we are in favour. We support a diversity of ways in which one's freedom to determine the fate of one's information may be sustained (the German concept of *informational self-determination*).

Privacy is not an absolute, it never was; it is not a matter of either/or — this value or that. A balance must usually be struck somewhere along the continuum between an absolutist position of total privacy and complete anonymity vs. one that denies or negates all privacy rights. While this view recognizes that personal privacy is valued as a fundamental right, deserving of the highest protection, it also recognized that at times, personal information is used in ways that may be considered comparable to a commodity or a currency. That is to say, personal information is often traded or exchanged for goods and services, sometimes at the behest of the individual, but far too often without his or her knowledge or consent.

The extraordinary growth of the role of technology in modern life (in particular, the World Wide Web) is arguably the principle reason for the commodification of personal information, transforming it into a key to unlock services of all kinds. It is said that the vast potential of electronic commerce requires, on the most basic level, this exchange of information. Yet it is becoming equally clear that electronic commerce will not reach the dizzying heights projected unless privacy forms a cornerstone of the e-business model.

Table of Contents

Executive Summary i

Abstract iii

Introduction 1

Human Rights, Ethics, and Privacy 4

Legislation vs. Self Regulation 8

Markets and Privacy 12

Individual Choice 12

Individual Choice in the Public Sector 13

Nature of Existing Market for Privacy 14

Structured Markets for Privacy 18

Ownership of Personal Data 18

Information Property Rights 18

Privacy-Enhancing Technologies (PETs) to Enhance Choice 22

Conclusion 26

Introduction

The privacy landscape in North America has been significantly recast in the last decade, the result of a shift in public perception that privacy, far from being an issue that almost exclusively engaged the public sector, now also preoccupies the private sector. For much of the period of the 1970s and 1980s, the focus of privacy concern was on government's potential, and often real, ability to engage in intrusive activities. This perception has now changed. As Ann Wells Branscomb, a highly respected privacy scholar, stated:

> Historically, our concern about computers was Big Brother -- the government invading our lives and having too much knowledge about and control over what we're doing. Now we're discovering that big business is the real Big Brother.[1]

This shift in concern has prompted a flurry of activity with respect to privacy.

> "Privacy" is among the most hotly debated topics in Washington and other national capitals today. Almost 1,000 of the 7,945 bills introduced in the 104th Congress addressed some privacy issue, and this level of political activity is reflected throughout much of the world, especially in Europe, where members of the European Union are busy implementing the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Privacy is the subject of thousands of scholarly and popular books, articles, position papers, reports, Internet Web pages and discussion groups and newsletters. The debate over privacy protection has spawned an astonishing array of industry and academic conferences, working groups, public interest and lobbying efforts, public surveys, and news stories.[2]

One should not be surprised that in the wake of this altered privacy landscape, the articulation of privacy issues and their resolution has also shifted. The framework for discussing privacy issues now encompasses a private sector commercial perspective, in addition to the traditional human rights and ethical approaches.

The aim of this paper is to explore these different perspectives, but particularly the private sector, or 'market' approach to privacy.[3] Can any insights gleaned from this approach provide a viable set of policy prescriptions for resolving privacy issues? Of particular interest is the outcome for individual control and personal choice if a market framework for

---

[1] Anne Branscomb interviewed in *CIO* magazine, February 15, 1996 <http://www.cio.com/archive/cio_021596_qa.html>.

[2] Fred H. Cate, *Privacy in the Information Age*, Brookings Institution Press, Washington, D.C., 1997.

[3] Some of the scholars associated with the market approach include: Eli Noam, Kenneth C. Laudon, Hal Varian, Peter Swire, among others. Their views are collected in a paper issued by the U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Washington, D.C., 1997.

protecting privacy was to be adopted. Can privacy issues be resolved by relying on the economic self-interest of individuals to make the appropriate decisions as to the degree of privacy that should be provided?

The perspective taken in this paper is the following: to the extent to which these different approaches can strengthen an individual's capacity to control the flow of his or her personal information and his or her ability to make choices about the collection, use and disclosure of his or her information, we are in favour. We support a diversity of ways in which one's freedom to determine the fate of one's information (informational self-determination) may be maintained.

Privacy has become a mainstream public policy issue, one that gives every indication that it will preoccupy policymakers well into the next century.[4] That privacy issues have attracted so much attention among so many diverse individuals, groups and organizations in different countries owes in no small measure to the growing impact of information technologies on our day-to-day life. Moreover, the extraordinary growth of the Internet (Net), especially the World Wide Web (Web), has further increased this concern, particularly since it has shown itself capable of becoming the platform for electronic commerce. As a new way of doing business, it is generally recognized that electronic commerce will not become commercially successful unless personal data collected as part of the electronic transaction (transaction-generated data) are strongly protected.[5]

During the 1990s, it became increasingly apparent that with the proliferation of computer databases and 'data warehouses' in both private and public sectors,[6] and with the rise in popularity of the Web, the previously benign view of the private sector's handling of personal information could no longer be sustained. For the private sector, personal information has indeed become a commodity — something to be collected, used and exchanged to ensure greater profitability and competitive advantage. Early evidence also indicates that personal data obtained in transactions conducted over the Web can be a further source of commercial value. Yet, it is this very commodification of personal data that has become the focus of much public attention and debate. As a practical business decision, collecting, using and even selling personal information can make sense, since such information is abundantly available, and at relatively little cost. Yet, the treatment of personal information by businesses does not always accord with the wishes of the individual concerned.

---

[4] With the European Union as the principal international driver of this issue, most developed countries are being forced to contend with privacy in the context of electronic commerce. For an overview of these international developments, reference should be made to the activities of the Organization for Economic Development and Cooperation <http://www.oecd.org/dsti/sti/it/index.htm); European Union <http://europa.eu.int>.

[5] In the U.S., the Clinton Administration's *A Framework for Global Electronic Commerce* makes this point <http://www.iitf.nist.gov/elecomm/ecomm.htm>, as does the report by the Task Force on Electronic Commerce, Industry Canada and Justice Canada, *The Protection of Personal Information: Building Canada's Information Economy and Society*, January, 1998 <http://www.strategis.ic.gc.ca/sc_mrks/privacy/endoc/homepage.html>.

[6] The impact of data warehousing and data mining is explored by Robert O'Harrow Jr, "Are Data Firms Getting Too Personal," *Washington Post*, 8, 9, 10 March, 1998.

While informational privacy has never been easily defined, a core concept of most definitions is the notion of control — that individuals possess the ability to control the uses of information relating to themselves. Implicit in this definition is the idea that in exercising such control, individuals can also make choices about the boundaries of their privacy.[7] Freedom of choice is critical to privacy. People should be able to decide what personal information they choose to reveal, how much they wish to reveal, and to whom. In other words, one could say that they should possess, as they do in some jurisdictions such as Germany, 'informational self-determination.'[8] Negotiating this boundary takes place informally in one's private life; however, in the public sphere, informal and consensual negotiations about informational privacy are more problematic, as we shall see.

Our focus in this paper will be on informational privacy in the public sphere – that area of life where individuals enter into institutionalized relations with others, whether that be in the workplace, in relations with government, as members of organizations, in the context of economic and service-related transactions.[9] To be clear, *the public sphere includes both private and public sectors.*

We will begin with a discussion of how the existing perspectives relating to privacy, human rights and ethics contribute to an understanding of privacy issues and their solutions, and how these perspectives are incorporated into the two primary ways of dealing with privacy, namely, through legislation and self-regulation. Then we will turn to our main focus of interest in this paper, the market-based approach.

---

[7] Rohan Samarajiva has defined privacy "as the capability to implicitly or explicitly negotiate boundary conditions of social relations." "Privacy in Electronic Public Space: Emerging Issues," *Canadian Journal of Communication* <http://www. ccsp.sfu.ca/cjc/BackIssues/19.1/samaraj.html>.

[8] For a discussion of the impact of the German Supreme Court decision that defined information self-determination and European developments generally see, Viktor Mayer-Schonberger, "Generational Development of Data Protection In Europe," in Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge Mass., 1998.

[9] A discussion of why privacy should be analysed in institutional settings is provided by Philip E. Agre, *The Architecture of Identity: Embedding Privacy in Market Institutions*, draft version September 1998 <http://www.dlis.gseis.ucla.edu/pagre/architecture.html>.

Human Rights, Ethics, and Privacy

One would not succumb to an overly broad generalization if it were claimed that the mainstream theoretical perspective on privacy has derived from the human rights tradition. While it is unlikely that this approach will be superceded, other perspectives also exist.[10] As we shall explore later, a market approach, based on economic theory, appears to be gaining strength. Before turning to this, a review of the human rights perspective may be useful as a counterpoint.

What has been compelling about the human rights approach is that it acknowledges privacy as a moral and social value. Privacy possesses moral value since, it has been argued, privacy supports the development of individual dignity and autonomy.[11] As stated by the Standing Committee on Human Rights and the Status of Persons with Disabilities: " Privacy is a core human value that goes to the very heart of preserving human dignity and autonomy."[12] It also furthers broader societal goals that augment the general social welfare.[13] In practical terms, respect for privacy requires those in the public sphere to take individuals' privacy into account in various interactions and transactions. This can be accomplished through the adoption or observance of a set of rules on how personal information should be dealt with, and consensus exists that this set of rules, at a minimum, should consist of what are commonly referred to as fair information practices.[14] By prescribing such rules, they are implicitly made to apply in all contexts where personal information is collected, used or disclosed. These fair information practices essentially set out informational privacy rights, providing a framework for an interactive relationship between the individual and the organization that is collecting, using, or disclosing one's personal information.

The human rights approach to privacy has been buttressed by a variety of international human rights covenants that, by recognizing privacy as one of the fundamental human rights, endows all individuals with a moral claim to privacy.[15] Such covenants include: the *Universal*

[10] The literature on privacy has become too vast to be provided here. A good start would be the Web pages of such bodies as the various privacy commissioners that operate in Canada at the provincial and federal levels, as for example, the Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca>. As well, the U.S. House of Representatives Web page dealing with privacy and access to information issues <http://www.house.gov/107.htm>.

[11] For a succinct review of the arguments favouring privacy as a social value, see, Cate, *op.cit.*

[12] Canada, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Third Report*, 1997 <http://www.parl.gc.ca?committees352/huso/reports/03_1997-04/app1e.html>.

[13] Reference here is not to the generally accepted economic notion of general welfare that rests on economic efficiency arguments, but on social notions of welfare that rest on the creation of social relationships based on trust, compromise, and respect.

[14] "Fair information practices" were articulated internationally in 1980 when the Organization for Economic Cooperation and Development issued its document, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, and consist of a number of privacy or data protection principles.

[15] For a discussion of privacy in the human rights context, see Jamie H. Lyford, "The Ministry of Truth Redefined: A Consideration of Privacy and Data Protection Law with Specific Consideration of the Role of International Human Rights Law," *E Law*, Murdoch University Law School, 1994 <http://www.murdoch.edu.au/elaw/issues/vIn3/lyford.txt>.

Declaration of Human Rights (1948), the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (1950), and the *International Covenant on Civil and Political Rights* (1966). By adopting these covenants, the international community has registered its conviction that privacy is a value that society as a whole needs to protect. Implicit in this judgment is the view that privacy provides benefits to society by strengthening an individual's capacity for autonomous action and thought. In the process, society gains the benefit of responsible individuals who respect the moral claims of others, and in the process, raises the general well-being within society. A human rights approach to privacy invites the adoption of uniform and universal rules for protecting informational privacy.

One would expect that since most governments are signatories to these declarations and covenants, the principles they espouse would have been translated into national laws. Yet, in the North American context, neither the United States Constitution, nor the Canadian Charter of Rights and Freedoms explicitly protects privacy, though in each jurisdiction the courts have recognized an implicit right to privacy under certain circumstances that emanate from their respective constitutional enactments. This implicitly defined 'right to privacy,' however, is narrow and exclusive in scope. Broadly defined, privacy is not explicitly protected.[16] In the Canadian context, the limited scope of a right to privacy in the Charter of Rights and Freedoms has prompted some to argue for the adoption of quasi-constitutional protections that would be subsumed under a Privacy Charter, applicable to both the public and private sectors.[17]

Some provincial and state jurisdictions in Canada and the U.S. have adopted tort (civil) laws for invasions of privacy that give individuals a cause of action with respect to invasion of privacy. At the same time, governments in North America have adopted an ad hoc or patchwork set of laws for protecting privacy, concentrating largely on informational privacy or data protection. Thus, data protection laws have been adopted by all federal and most provincial public sectors (and some states), as well as for some specific business sectors.

From the individual's perspective, this patchwork of laws leaves a fragmented legal terrain that burdens, and possibly overwhelms, an individual's ability to protect his or her privacy. As a result, in many different interactions and transactions, the individual is left in a one-on-one relationship with an organization to determine what legal rules apply through which the individual can exercise some control over his or her informational privacy.

If the human rights perspective posits that all humans have a moral claim to privacy, the ethical question is how should individuals behave to further this claim, or, more properly, what is the best behaviour that should be adopted to protect one's privacy? However, since our initial

[16] In the Canadian context, these issues are raised by Valerie Steeves, "Humanizing Cyberspace: Privacy, Freedom of Speech, and the Information Highway," Human Rights Research and Education Centre, University of Ottawa, June 1996 <http://www.uottawa.ca/~hrrec/publicat/cyber95e.html>. For the American context, see, Susan E. Grindin, "Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet" <http://www.info-law.com/lost.html>.

[17] In 1997, the Standing Committee on Human Rights and the Status of Persons with Disabilities issued its report, *Privacy: Where Do We draw the Line?*, in which it argued for a privacy charter for Canada.

assumption was that we would look at privacy in the public and not the private sphere, our question must be reformulated — how should organizations, associations, companies, groups, etc., behave in order that personal privacy may be protected?

Ordinarily, in dealing with collective entities, ethical concerns about individual behaviour in those organizations have been framed in the context of codes of conduct. Such codes have been adopted by a variety of organizations, industry sectors, professional bodies and companies.

Codes may either be obligatory rule-based ones that must be observed, such as those that pertain to many professional bodies, or they can take the form of guidelines adopted voluntarily, such as those adopted by numerous industry sectors and voluntary organizations. In the former case, a breach of the rules can occasion disciplinary action, while in the latter, it cannot.

A comprehensive breakdown of various types of private sector privacy codes has been developed by Professor Colin Bennett, who categorizes them under five headings:

Individual Company Codes — those that have been developed by companies in the absence of, or in anticipation of, the development of wider sectoral instruments (e.g., the American Express *Privacy Code of Conduct*).

Sectoral Codes of Practices — those that have been negotiated by an industry group, recognizing the need for consistency of policy and practice, while establishing a set of rules tailored to the needs of the industry and pre-existing regulatory framework for the sector (e.g., the Canadian Bankers Association's *Model Privacy Code*).

Functional Codes — those that have been defined by the practice in which the organization is engaged (e.g., the Canadian Direct Marketing Association's *Code of Ethics and Standard of Practice*).

Technological Codes — those that address specific potentially privacy-invasive practices involving information and communications technology (e.g., the bank code for the governance of electronic fund transfers).

Professional Codes — those that have been developed for use by professional societies and associations (e.g., the Professional Marketing Research Society of Canada's *Rules of Conduct and Good Practice*).[18]

From the perspective of the individual whose privacy may be at stake, he or she must rely on an organization's ability to instill the required ethical code of conduct and judgment in its members and employees. If such rules are not embedded in the organization's way of doing business (or its corporate culture), employees will likely rely on their own behavioural models

[18] Colin J. Bennett for the Canadian Standards Association, *Implementing Privacy Codes of Practice*, PLUS 8830, August 1995, pp. 18–21.

(which may not always be consistent with a formally adopted code).[19] At times, the weakness of such codes is that they are adopted *pro forma*, with no real attempt by senior management to instill the rules into the organization.[20] Under these circumstances, the individual consumer can seek to remind the organization of the obligation it has entered into by adopting a code of conduct, but the individual must first be aware of the code or know the policy expected to be followed. The individual affected by this situation could be forced, under these circumstances, to educate the member(s) of the organization concerned – namely to take on the responsibility that the organization itself should have undertaken. While such monitoring and educational activity may be undertaken by some consumers, it is not likely, given the time and effort that would need to be expended to learn the rules, that this activity would be undertaken by most individuals.[21] At the same time, it would be prohibitively expensive for companies to bargain with each customer separately.[22]

In the last analysis, a company's adoption of a code of conduct would depend on its calculation of its self-interest. For example, would such a code make good business sense? Would a strict observance of a code of conduct have an impact on a firm's profitability? This issue could arise in a highly competitive sector with many firms seeking some advantage, relative to the others. If, for example, one firm is commonly selling personal information from its databases, this could exert pressure on competing firms that do not engage in this practice. However, a counter-balance would, in part, arise if there was a high public expectation of privacy. A significant cross-section of the public would, of course, have a greater impact on the adoption of codes than the concerns of a few consumers. Thus, the market power of a large segment of the public will have a greater impact on corporate behaviour than the asymmetrical power of a few individuals.[23] The irony is that while privacy protection is an individual concern, its effective enforcement may only come through collective action. Whether an aggregation of privacy concerns will coalesce at any given moment in time is difficult to predict. Until such aggregations develop, individuals will be left on their own to monitor and enforce existing codes of conduct.

---

[19] A recent Canadian survey was conducted to assess the level of awareness and knowledge of privacy laws and codes by frontline staff and how well they apply them when dealing with customers. The results indicate that, overall, employees at most organizations did quite poorly in their awareness and implementation of core data protection principles and standards that apply to their place of employment. Consumer Awareness Network and Public Interest Advocacy Centre, *The 1998 Personal Data Protection and Privacy Review*, May 1999. See also, Tracy LeMay, "Consumer privacy still minor issue - survey," *National Post*, May 26, 1999, p. D1.

[20] This issue is raised by Errol P. Mendes and Jeffrey A. Clark, "The Five Generations of Corporate Codes of Conduct and Their Impact on Corporate Social Responsibility," Human Rights Research and Education Centre, University of Ottawa, 1996 <http://www.uottawa.ca/~hrrec/publicat/five.html>.

[21] For a discussion of the issues confronting an individual as he or she tries to negotiate privacy with a firm, see, Peter P. Swire, "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Washington, D.C., 1997.

[22] On this point, see, Peter H. Huang, "The Law and Economics of Consumer Privacy Versus Data Mining," May 1998, Law School, University of Pennsylvania.

[23] This issue is explored by Mary J. Culnan, "Self-Regulation on the Electronic Frontier: Implications for Public Policy," in *Privacy and Self-Regulation in the Information Age*, op.cit.

Of course, individuals may choose not to do business with a company that does not have a code of conduct or one that does not adequately abide by its code. While this is clearly every individual's prerogative, it may well turn out that the individual is forced to deal with that firm nonetheless since any viable alternative service may not be available. Alternatively, the exercise of this prerogative may be academic if none of the relevant companies has a code of conduct.

Despite the shortcomings of the human rights approach in being translated into legislation, it is fair to say that it constitutes the mainstream position of those advocating for privacy protections.[24]

Legislation vs. Self-Regulation

The previous discussion highlighted the fact that governments in North America (especially in the U.S.) have been hesitant to bring forward *comprehensive* private sector legislation to protect privacy on the basis of human rights arguments and that while codes of conduct are the method of choice for dealing with privacy in the private sector, this approach is not without its problems with respect to the scope and enforcement of those protections.[25] More often than not, individuals are largely left on their own to protect their privacy.

Considerable debate has developed over the merits of legislation vs. self-regulation as the mechanism of choice for protecting informational privacy in the private sector.[26] Taking the debate on self-regulation in the U.S. as fairly representative, self-regulation rather than legislation is seen as the most appropriate mechanism to protect privacy on the grounds that legislation is too inflexible and time-dependent to be responsive to the fast-moving world of information technology.[27] It is feared that government legislation will likely lead to an overly bureaucratic and cumbersome regulatory process that will only result in raising the operating

[24] For a discussion of this point, see Colin J. Bennett, 'Privacy Protection Still Fundamentally Human Rights Issue,' *Government Information*, Vol. 3, number 1 (summer 1996) <http://www.Usak.ca/library/gic/v3n1/bennett/bennett.html>.

[25] These problems have been highlighted in the ongoing discussions between the European Commission and the U.S. Department of Commerce regarding the adequacy of the proposed "Safe Harbor" principles. The European Union is bound by the *EU Data Protection Directive*, while the Americans continue to support self-regulation. At the time of publication, the discussions remained deadlocked over the issues of data subject access and enforcement.

[26] A valuable reference source on self-regulation is *Privacy and Self-Regulation in the Information Age*, issued by the National Telecommunications and Information Administration, U.S. Department of Commerce, 1997.

[27] The debate in the U.S. is recounted by Jeri Clausing, "U.S. Report on Net Commerce Set for release," *New York Times*, 30 Nov. 1998.

costs of the businesses involved. While undoubtedly there is some merit in this claim, it cannot be denied that business has been very slow to adopt self-regulation, even though it is said to be its preferred course of action.[28]

For its part, the U.S. government has had to resort to threats of introducing legislation in its attempts to force companies to regulate themselves.[29] The indecisiveness of business does not auger well for the consumer. The end result could be a situation where some companies abide by self-regulation while others do not, leaving individuals confused as to what rights they may have, and whether they will have to determine what privacy policies exist, which firms have adopted them, how closely they follow them, and what options are available if redress is sought. Failure to adopt uniform and universally applicable privacy rules through self-regulation raises the issue of whether legislation is needed, at least to some extent, as the Canadian approach suggests, or legislation that requires the adoption of self-regulation.[30]

Self-regulation, as previously discussed, cannot be comparable to an organization adopting a code of conduct with respect to how it will deal with personal information. While such codes are commendable and to be encouraged as a way to create a corporate culture respectful of privacy, codes alone cannot be fully relied on. If they are voluntary, thus not universally adopted, individuals are compelled to expend considerable time and energy researching

---

[28] In the U.S., the extent of self-regulatory measures on the Web seems to be open to interpretation. As an example, the Online Privacy Alliance (OPA) issued a press release indicating that the Georgetown Internet Privacy Policy Survey, released in May 1999, showed that 65.7% of the visited Web sites had at least one type of privacy disclosure (i.e., notice or information practice statement). The same press release reported that the OPA's own survey showed that 94% of the top 100 Web sites had posted at least one type of privacy disclosure. The emphasis of the press release was that these results were a vast improvement over the Federal Trade Commission's 1998 survey that found only 14% of sites told consumers how the companies were using their personal information. One of the OPA's conclusions was that: "These surveys, taken together, show that industry is creating a well-lit thoroughfare on the Internet where consumers can feel safe ... Policymakers should recognize progress in self-regulation and not rush to regulate the Net in ways that could undermine electronic commerce." <http://www.privacyalliance.com/news/05121999.shtml>.

The Center for Democracy and Technology issued a press release about the same Georgetown survey announcing that the results indicated that only less than 10% of the privacy notices were meeting basic requirements called for by industry leaders, the Administration, the Federal Trade Commission, and the advocacy community. In that press release Susan Grant, Vice President of Public Policy at the National Consumer League, was quoted as saying: "It's time to stop asking if self-regulation alone will work. The right question for the FTC, Industry and Congress to ask is: 'How do we ensure that consumers' privacy is protected on the Net.'" <http://www.cdt.org/press/051299press.shtml>

[29] Theta Pavis, "Government Ready to Dictate Privacy Rules," *Wired News*, 26 March 1998 <http://www.wired.com/news/news/politics/story/11214.html>.

[30] In Canada, the *Personal Information Protection and Electronic Documents Act* (Bill C-54) is based on the model privacy code of the Canadian Standards Association. At the time of publication, it can be reported that Bill C-54 had been introduced into the House of Commons and was being debated when the House rose for the Summer. It is anticipated that consideration of the bill will resume when the House returns in the Fall of 1999. At the 18th International Conference on Privacy and Data Protection, held in Ottawa in September 1996, the Minister of Justice announced the Canadian federal government's commitment to have "federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector" by the year 2000. That commitment has been reiterated as the legislation has been developed.

which firms have codes and how effectively they are enforced. Therefore, irrespective of how individuals negotiate their privacy, the possibility remains that they may not be able to hold the firm to respect their choices.[31]

Self-regulation, as now commonly understood, means that a given business or industry sector establishes privacy rules among the firms that make up that sector.[32] Some have argued that such self-regulation, coming as it often does on the heels of government threats to introduce legislation, is in fact a form of government regulation, though administered, supposedly, less rigidly and less bureaucratically by business itself. For this to be valid, one would expect to see some of the same features in this type of self-regulation as in legislative schemes: a set of informational privacy rules based on fair information practices, a method of enforcement, and an independent oversight/dispute resolution mechanism.

The motivation for this form of self-regulation is the same as for government legislation. There is a need to equalize the asymmetries of information and bargaining power between individuals and businesses, allowing individuals to make choices in the context of established privacy rules.

These difficulties in the implementation of self-regulation, however, should not let us lose sight of the fact that self-regulation can be an effective way to protect privacy in the private sector. But, in order to be effective, certain base requirements must be in place. Self-regulation does not equal the voluntary adoption of codes of conduct by individual firms. Competitive pressures could force the implementation of such codes to the level of the firm whose profitability rested on not following such a code. Self-regulation means the adoption of a privacy standard across a given business sector so that intra-sector competition could not act

---

[31] In his paper, *Implementing Privacy Codes of Practices*, Colin Bennett correctly notes that self-regulation does not equate to voluntary. There exists a continuum of incentives for compliance amongst self-regulatory privacy codes. At the one end there are purely voluntary codes with no internal or external compulsion to develop, adopt or implement privacy standards. At the other end there are codes that are "interpretive instruments" designed to apply data protection legislative rules to specific industries. See, "The Extent of Compulsion" section of Chapter 2 of Bennett's paper.

Also, it should be noted that there are varying levels of oversight and enforcement with private sector privacy codes. The Canadian Standards Association (CSA) has the Quality Management Institute (QMI) recognition program which offers three tiers of recognition: 1) *declaration* of the organization's intent to apply the CSA Model Privacy Code; 2) *verification* by QMI that the CSA Code has been implemented to an acceptable standard; and 3) *registration* with QMI. For more details on these tiers and the role of the QMI, see the Canadian Standards Association publication *Making the CSA Privacy Code Work for You: A workbook on applying the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830) to your organization*, PLUS 8300, December 1996, as well as Chapter 11 of *Implementing Privacy Codes of Practices*. Another example is the enforcement procedures followed by the Canadian Direct Marketing Association (CDMA) when it receives a complaint regarding a potential violation of its *Code of Ethics and Standards of Practice* by a member. A copy of the CDMA code may be found on its Web site at <http://www.cdma.org>.

[32] The discussion on self-regulation here relies on the publication of the Data Protection Working Party of the European Commission, "Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?" January 1998 <http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.htm>.

as an impediment to the implementation of the protections set out. Another requirement would be that enforcement of the privacy standard should come through an independent entity outside of the business sector to which the standard applied. Finally, complete information about how the standard would operate within the given business sector and the mechanisms for redress should be made broadly available to the public. Such openness and transparency should have as its objective the reduction of cost to individuals for acquiring the necessary means to exercise control over their personal information.[33]

[33] Swire, *op.cit.*, provides a useful discussion of the characteristics of effective self-regulation.

Markets and Privacy

While the human rights approach to privacy has served as the principal theoretical underpinning of privacy advocacy for the last several decades, it has been challenged, from time to time, by a market-based approach. One of the distinguishing characteristics of this approach is the reliance it places on individual choice as the locus of decision making about privacy. While data protection laws create a formal administrative framework for the protection of personal information, they do not encourage individuals to take an active role in the protection of their own personal information.[34] The arguments in favour of various market-based approaches rest on creating the conditions that would allow for individuals to be more proactive in making choices relating to the flow of their personal information.

Individual Choice

Defining what we mean by choice is not always an easy task. Several different but related notions are often intermingled.[35] Is making a choice a question of deciding between alternatives, or is it the very act of making a choice? Alternatively, is it raising the value of the choice made? Ordinarily, most individuals tacitly understand that in making a choice, the process of making the decision is important; however, they will most likely concentrate on the object of their choice and will seek to raise the value of that choice in the process.

For our purposes, we define choice as the freedom to choose among alternatives or options, on an informed basis, and in the absence of coercion. Needless to say, the alternatives should all be positively valued, so that something valued need not be sacrificed in order to obtain something else of value. Implicit in making decisions is the requirement that the individual have sufficient knowledge or information to be able to make an informed choice. Several assumptions also warrant articulation in the context of informational privacy: personal information is viewed by individuals as belonging to them — they are the rightful 'owners,' and, this being the case, they feel they have the right to decide if they will disclose it, and to whom. Individuals generally value their privacy and wish to protect their personal information from being collected, used or disclosed by others, absent their consent.

The context in which individuals make their choices can have a direct bearing on the efficacy of the choice. In institutional settings, an individual is dependent on access to information that would allow him or her to make an informed choice. At the same time, the relative bargaining power of an individual in relation to the organization could affect the choice made. A weak bargaining position could lead the individual to choose a privacy option that may not be optimal nor serves the individual's best interests. This predicament is highlighted in an individual's dealings with the state.

[34] The 'free rider' problem can arise in those circumstances, when individuals rely on the active involvement of others to gain the benefits of such activity for themselves.

[35] The discussion on choice relies to a large extent on the analysis of Keith Dowding, "Choice: Its Increase and its Value," *British Journal of Political Science*, Vol. 22, pp 301–314.

Individual Choice in the Public Sector

In the context of the public sector, an individual's ability to negotiate the boundaries of informational privacy and exercise some choice is circumscribed by the state's coercive power, which can compel individuals to act as prescribed by law. We are, for example, required by law to provide certain personal information as a condition of receiving a government benefit or being certified to perform a certain function (such as driving a motor vehicle). We can say that under these conditions the individual has *asymmetrical bargaining power*, the individual has little or none, while the state possesses a monopoly.

In advanced democracies, various measures have been taken to curb this coercive power, ranging from constitutional enactments to ordinary laws. Thus, most western liberal democracies have adopted laws that bind governments to observing fair information practices. Ideally, one would want to have privacy rights grounded in a constitutional enactment, rather than subject to ordinary law. Absent such legal constraints on the state, an individual would have few mechanisms available to control how the government might collect, use and disclose his or her personal information.

From the perspective of individual choice, while recognizing the limits that laws intrinsically place upon individuals, the extent to which governments do, in fact, adopt fair information practices can be said to provide some measure of privacy protection. Thus, while individuals may be compelled to provide personal information to government in the first instance of collection, they can exercise a measure of control thereafter. Thus, consent is required of the individual when personal information is used for another purpose within government and when it is disclosed to someone outside of government. Moreover, limitations are placed on the collection of personal information, restricting such collection to lawfully authorized ones that have specifically identified purposes.

In transactions between the individual and government, an individual can rely on data protection legislation to ensure that government agencies treat his or her personal information consistently across government, according to fair information principles that enhance his or her control over that information and permit a measure of choice as to how it will be treated. Individuals also have the right to make complaints to an independent oversight agency (in Canada) or to the courts (in the U.S). The adoption of data protection laws obviates the need by individuals to acquire detailed information on how specific government agencies treat personal information in order to monitor government actions. Individuals can place some measure of trust in government to uphold the law and in independent oversight bodies to resolve disputes and hold government to account for how it deals with personal information. Thus, asymmetrical bargaining power between individuals and the state can be held in check through such measures. However, even with all these legal norms and practices, government failure to observe these rules and practices can and does occur.

Given the state's coercive power, few would argue that privacy laws should not govern how the state treats personal information. Yet, from the perspective of individual choice, an individual's relations with the state do not provide the optimal conditions for exercising choice.

Nature of Existing Market for Privacy

The private sector, on the other hand, is recognized as not possessing coercive powers comparable to that of the state that can compel individual behaviour. Rather, economic theory posits the notion of consumer sovereignty which asserts that individual consumers possess the ability to choose which products and services they will buy and, thereby, determine what goods or services will be offered in the marketplace.

Economic theory makes no normative assumptions about privacy as a social value. Whatever value privacy may have for individuals, this will be determined by each individual's utility preferences. Where privacy will be placed in this value hierarchy is a matter of individual choice. In the final outcome, if this rational calculation of value is applied, individuals would set the price of their personal information in competitive markets that, in theory, should permit individuals to obtain the level of informational privacy most desirable to them, and permit businesses to obtain the optimal volume of personal information in order to carry on commercial transactions. An inherent assumption of the market approach is that companies have a legitimate interest in acquiring personal information for business purposes, and this should not be arbitrarily restricted.[36] It is said that an individual's interest in protecting his or her personal information should be matched by the interest of businesses to acquire personal information.

However, looking at the situation that prevails now, one can say that an 'unstructured' market for privacy exists, with few rules as to how personal information should be dealt with in the marketplace. While personal information has been commodified or commercialized, there has not been a corresponding empowerment of individuals that would give them the ability to control how their personal information will be used, or for which they will be compensated. Companies can now freely collect, use or disclose personal information without having to pay any compensation or, in many instances, without having to abide by any privacy principles such as those found in fair information practices.[37] Instead, personal information now has some of the characteristics of a 'public good,' and as such, is widely available.[38] In this unstructured market, there is no legal mechanism that individuals can rely upon to secure their right to enjoy 'exclusivity' to their own personal information, much as they do with other personal property that they presently own.

---

[36] Eli M. Noam argues that private firms should have the legal right to contact an individual to obtain personal information, in addition to the individual having a right of property to his or her own information, See, "Privacy and Self-Regulation: Markets for Electronic Privacy," in *Privacy and Self-Regulation in the Information Age*, issued by the National Telecommunications and Information Administration, U.S. Department of Commerce, 1997.

[37] Both in the U.S. and Canada, various laws exist at the federal and state or provincial levels that require designated business sectors to abide by fair information practices to some degree. A listing of such U.S.laws can be found in Eli M. Noam, "Privacy in Telecommunications: Markets, Rights and Regulations," manuscript, 1993.

[38] Characteristics of a "public good" are its non-excludability and non-depletability. "My possession of a good does not limit your ability to also possess it, nor is it depleted if I consume it. The most used example of a public good is the air we breathe." W. Curtis Priest, *The Character of Information: Characteristics and Properties of Information Related to Issues Concerning Intellectual Property*, Office of Technology Assessment,1994.

Information may be used and disclosed endlessly. One has only to look at the so called 'look-up' services that can assemble a dossier on individuals by relying on various databases, to see how freely available personal information truly is.[39] Under these conditions, an individual's ability to exercise control and have real choice about how his or her personal information may be used is severely limited. From the individual's perspective, one's ability to exercise control over one's information in this situation is significantly limited due to, as economists would say, 'asymmetrical information and bargaining power.'

Asymmetrical information refers to the imperfect knowledge or information that consumers may have about a product, the company that made the product, alternative products, and so on when they enter the marketplace. Asymmetrical bargaining power refers to the relative market power of one individual to make a difference in the behaviour of a business, as to price, quality or service. In combination, both these asymmetries place the individual at a disadvantage relative to a business when individuals assert their consumer rights. Applied to our privacy context, individuals would need to have fairly detailed information about the behaviour of businesses and the value of their personal information to their operations to determine how their information will be handled and what commercial value it may possess. To acquire this knowledge for all the transactions an individual engages in over the course of time would require a great investment in time and energy. Ordinarily, individuals calculating their self-interest are unlikely to invest such time and effort into acquiring the necessary information to be sure of a company's privacy policies. If individuals consider the privacy implications inherent in any transaction, they will likely infer a level of trust in the relationship that will obviate the need to acquire the necessary information to confirm (or remove) their placement of trust. Long-established relationships would likely be given preference in any decision calculation in order to discount the issue of trust.[40]

There has been a sufficient number of reported episodes of companies abusing their customers' personal information to indicate that such trust can be misplaced. In some instances, individuals have been able to aggregate their objections to a company's handling of their personal information to affect a change in the particular company's behaviour. But such aggregation of concern that actually leads to changes in business behaviour is rare and owes to the uniqueness of the particular situation. The most commented on instances have related to the use of Internet e-mail capabilities to create a coalition of like-minded individuals

[39] The U.S. Federal Trade Commission was sufficiently worried about the activities of these "look-up services" or individual reference services to issue a report to Congress recommending action to limit their privacy intrusive activities. The firms in this sector eventually decided to regulate themselves. For the report see, Federal Trade Commission, *Individual Reference Services*, December 1997 <http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm>.

[40] For an interesting discussion of some of these points see, Rohan Samarajiva, "Interactivity: As Though Privacy Mattered," in Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge Mass., 1998.

who are prepared to confront a given business.[41] Ordinarily, individuals would need to confront a company on an individual basis, and under these circumstances, any negotiations an individual would enter into about the handling of one's personal information would issue from a distinct disadvantage: the individual would have an asymmetrically lesser ability to affect the company's behaviour than if he or she were part of a larger group. Market power resides in large numbers of customers willing to voice their objections to a company's privacy policies. The logical conclusion to be drawn from this predicament is that the bargaining position of individuals should be equalized relative to businesses and that information about a company's privacy policy should be made readily accessible.

Under existing market conditions, it would appear that individuals are presently at a disadvantage in being able to control or negotiate the boundaries of their informational privacy. One solution is to introduce privacy legislation to cover the private sector. The argument for such legislation would not turn so much on the market's coercive power, but on the present unstructured market's failure to adequately satisfy individuals' ability to exercise control over their personal information. While this is the theoretical justification for such legislation, a closer look at what happens in the marketplace may invite us to reconsider the issue of coercion.

Upon entering the marketplace, individuals frequently have to provide some personal information to complete a transaction. In some cases, that information is incidental to the transaction, while in other cases, it may be central to the transaction. Ordinarily, the individual would provide sufficient personal information to complete a given transaction. In effect, the individual is implicitly consenting to the collection of personal information by a given company, with the understanding that the purpose of the collection is to perform and complete the transaction at hand.

Another way of looking at the initial collection of personal information is to view it as a question of choice, where the choice is either between two positive values, or a positive and a negative value. In this case, the individual, who values both privacy and the product or service desired, would prefer to choose both, but must give up a small measure of privacy to complete the transaction. This 'Catch 22' situation may be quite acceptable to most consumers, if the collection of personal information is limited to that which is functionally necessary to complete the transaction.[42] However, if additional details are sought that do not

[41] "For example, America Online experienced a public relations nightmare when it attempted in mid-1997 to quietly amend its "Terms of Reference," which had stated that AOL would not reveal members' personal information to third parties. Once the amendment, which provided that AOL might make telephone numbers of AOL members available to AOL partners for telemarketing, was discovered, AOL received an onslaught of complaints from AOL subscribers, politicians and privacy-rights groups, and as a result, abandoned its plans." Susan E. Gindin, "Creating an Online Privacy Policy," October 1998 <http://www.info-law.com/create.html>.

[42] Jerry Kang argues that there should be a default position under these circumstances that would permit firms to collect only that personal information that was functionally necessary to complete the transaction. "Information Privacy in Cyberspace Transactions," *Stanford Law Review*, 1998, vol. 50.

appear to be functionally necessary, the consumer may well refuse to provide the additional information requested. The consumer has expressed his or her choice and has set a boundary to his or her informational privacy. At this point, the company may well accept the choice made or may seek to condition the purchase on the provision of the additional information. Such behaviour by the company would be considered unethical since the purchase would arise from a coercive action on the part of the company to acquire further information not required for the completion of the transaction.

One of the most contentious issues in the private sector is that of secondary use — businesses selling personal information to, or exchanging with, third parties, without the knowledge or consent of the individuals involved. This practice has become a lightening rod for consumers. Companies have a financial interest in being able to sell personal information and want individuals to accept this practice as appropriate to the marketplace, arguing that better customer service will be the end result. Individuals' acceptance of this practice is usually inferred when they are given, in some cases, a voluntary ability to opt-out of any database or list of names that could be sold to third parties, but fail to do so. When most individuals do not take this opportunity to say no (which in many cases could be the result of inadequate information or a poorly visible opt-out clause), companies feel free to sell their information to third parties. Fair information practices would require that individuals be asked to consent to such a disclosure (or sale) at the time this was contemplated. In this situation, a company's practices with respect to the treatment of personal information are not the result of any negotiation with individuals determining their best options. Rather, individual choice is inferred.

These examples would suggest that under conditions of asymmetrical information and bargaining power, individuals can be placed in situations where they have to make decisions under some compulsion, or put differently, individuals do not have a completely free choice in making decisions about their informational privacy.

Unquestionably, compulsion under these circumstances is different from what prevails when individuals are required to deal with the government. In the latter case, they often cannot exercise the option of exiting from the transaction, lest they break the law. In the business context, an individual can usually exit the transaction without any legal liability. Nonetheless, it is often the case that in most business transactions, an individual cannot choose to receive goods or services without providing some personal information. The clear exception is when the transaction is conducted anonymously, as, for example, when someone chooses to pay for a product with cash.[43]

[43] The issue of anonymity is discussed further in this paper in the context of Privacy-Enhancing Technologies and the new options available to online consumers.

Structured Markets for Privacy

The present unstructured market for personal information leaves the individual without any effective tools to assert his or her privacy rights. The consequences of asymmetrical information and bargaining power mean that individuals are largely powerless to influence the privacy policies of most businesses. Under these conditions, several scholars have argued for a *structured* market approach to protecting personal information.[44]

Their contention is that since personal information is a commodity, it should be exchanged in a well-structured market. These authors start with the assumption that different individuals value their privacy differently, with some not valuing it at all. Thus, they contend that a more realistic choice set is not just one where an individual chooses privacy and also a product or service, but a choice that includes obtaining the product or service *and* a measured loss of privacy. This view is held on the following basis: that in a true marketplace, individuals may choose to give up some of their privacy if they were adequately compensated for their loss through market-based mechanisms. And just how would this work? — through the creation of information property rights.

Ownership of Personal Data

First, one must establish ownership in property in order to assert rights of property. We maintain (as do the majority surveyed) that personal information belongs to the individual to whom it pertains: the data subject is the rightful owner of any personally identifiable information relating to him or herself. Once the issue of ownership has been determined, then full property rights of ownership can follow, as well as legally enforceable claims to the ownership of one's data.

Information Property Rights

Viewing an individual's personal information as an extension of his or her property does not require a great leap in logic. Property has been described as a legal relationship between a person and a "thing," wherein the thing may be physical or abstract (as evidenced by *intellectual* property). Property has been described as a "bundle of rights with different sticks in the bundle."[45] These rights include the right to use the property as one wishes and to exclude others from doing so, to alter its configuration, to enjoy its fruits including its income, and not least, to transfer the title of ownership.

When one considers the fact that the rights of property holders are embedded in the constitutions of most free nations, one can discern a similar direction for the treatment of personal information. Indeed, some have argued that "privacy cannot be attained without an

[44] For example, Tom Bethell, *The Noblest Triumph*, St. Martins Press, New York, 1998.

[45] Bethell. pp. 19–22

anterior respect for private property."[46] Given the relationship in the balance of power between the individual and the state, one can see how this would develop: "Property rights are held against the state — property is an important bulwark against state power, and like all genuine rights, property rights protect the weak against the strong."[47] In the same respect, privacy rights in this context, as a direct extension of property rights, could also protect the arguably weak (individuals) against the strong (government and business).

The mechanism by which this would be realized would be through the use of existing rules of property law, already on the books. One benefit would be that since property laws extend back for centuries, a large body of precedent is already available. Nobel Laureate Ronald Coase argues (as cited in Bethell), "when property is privatized and the rule of law is established in such a way that all the rulers themselves are subject to the same law, economies will prosper."[48] Adding personal information to the umbrella of existing property rights could perhaps similarly lead to such benefits in the nascent cyber-economy. The notion of information as property, however, is not new, dating back to the time of Warren and Brandeis.

The "how to" of it would take place as follows. Property rights to personal information would be assigned to the individual to whom the information related. The effect of assigning information property rights to individuals would eliminate the 'common good' characteristics that personal information now possesses. Instead, personal information would become a 'scarce good,' with commercial value. And, as a scarce good, personal information would be bought and sold through a price-setting mechanism that allowed individuals to find an appropriate price at which they may wish to sell, and offer businesses the right price at which they may wish to buy.

James B. Rule, an American scholar who has written extensively about the need for privacy, has advocated the adoption of this approach for several years. He argues that under present conditions, there is a high cost to be paid for the commercial erosion of privacy, and that in the United States at least, there has not been an adequate legislative and policy response to the issue of privacy. Rule believes that this has led to the existing situation where personal information is commercialized, forcing individuals to counter various intrusive practices on their own.

Rule's answer is for legislators to create a property right that would cover the commercial uses of personal information. Under this regime, express permission from the individual would be required before personal information could be sold or disclosed. In his view, no new government agency would need to be created.[49] Rule envisages that modest royalties would

[46] Bethell. p. 10

[47] Bethell. p. 10

[48] Bethell. pp. 316–317

[49] James B. Rule, "Privacy in an Information Age," *The Christian Science Monitor*, 6 Oct.1998; Another scholar arguing in the same vein is Eli. M. Noam, "Privacy in and Self-Regulation: Markets for Electronic Privacy," in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Washington, D.C., 1997.

be paid to those holding rights to their personal information, much like royalties are now paid to individuals or businesses for the use of some asset, such as royalties paid to musicians when their songs are played on the radio. Special agencies would be created that would seek to obtain the best royalties for their clients, much like CANCOPY (Canadian Copyright Licensing Agency) and SOCAN (Society of Composers, Authors and Music Publishers of Canada) do for authors, musicians and publishers.[50]

Another American scholar, Kenneth C. Laudon, has gone one step further and has proposed a structured market for the sale of personal information, which would "be based on individual ownership of personal information and a National Information Market (NIM) in which individuals can receive fair compensation for the use of information about themselves."[51]

Several assumptions are made by Laudon in arguing for a market-based approach to privacy, one of which is that in the new world of information technology where transaction costs can be significantly reduced, information, including personal information, can flow much more readily. At the same time, the economic system in large measure has become dependent on this flow of information. Privacy under these conditions can be viewed as a hindrance, since by keeping to strict privacy principles, personal information would not be permitted to circulate at all, or at a high cost. On the other hand, the fact that under present-day arrangements, users of personal information seem to effectively 'own' the information, tends to lead to its overuse, since the users need not obtain the permission of the individuals concerned. "Once individuals lose control of information about themselves and ownership of the information, the information is then used freely by other institutions to market and communicate with and about individuals."

Laudon calls for the creation of a National Information Market in which information about individuals would be bought and sold at a market clearing price, freely arrived at, in which supply equals demand. This market would be based on secondary and tertiary uses of the information.

Under Laudon's scheme, individuals would establish information accounts and then deposit their personal information, their 'assets,' in a local information bank, possibly a financial institution. In turn, the information bank pools the depositors' personal information in 'baskets' containing various types of personal information, medical, credit and so on. These baskets of personal information would be sold on a National Information Exchange. This acquired personal information could then be used for commercial purposes. Payment for the use of the information would go back to the local information bank, which would compensate individual accounts for the use of the information. Private placements could also be made by those willing to sell their information for commercial purposes, with payment assured through a National Information Accounts Clearinghouse. If individuals felt that they did not have the time or interest to participate directly in such a market, information agents would likely appear, willing to broker individuals' personal information on the market, seeking to

[50] Lawrence Hunter and James Rule, "Toward Property Rights in Personal Information," manuscript, 15 Jan. 1994. The paper is now published in *Visions of Privacy: Policy Choices for the Digital Age*, ed. Colin J. Bennett and Rebecca Grant, University of Toronto Press, 1999.

get the best price (see "Infomediaries," page 22). The asymmetrical information deficit that individuals may be prone to could be offset by their reliance on such agents.

Of course, such a market for personal information would not have as its first objective the regulation of privacy abuses or the enhancement of privacy, but rather, an economically more efficient flow of personal information throughout the economic system. The dilemma for the individual would be in making the decision whether or not to participate in such a market. This clearly would be a matter for individual choice, as would the setting of each individual's privacy preferences.

Another American scholar, Eli M. Noam, has also speculated as to what sort of privacy transactions would take place where there was an initial allocation of rights: an individual would possess property rights in his or her personal information, while a company would have the right to call up the individual to obtain his or her personal information. In effect, there would be a distribution of rights between individuals and firms, with each gaining a right that could be used in the marketplace. Under these conditions, the individual and the company would bargain for their interests, with the company having to pay compensation if it wanted to obtain the individual's personal information. According to Noam, whether there would in fact be a transaction would depend on several factors: sufficiently low transaction costs; a legal environment that permitted the transaction; a compatible industry structure; symmetry of information among the parties; no market failure, i.e., no instability in the market, and finally, a property right in personal information.

Taking these factors as the basis for his analysis, Noam then looked at several sectors where privacy was an issue: telemarketing, mobile eavesdropping, databanks and corporate networks. He concluded that markets would work in the first two cases, but not in the last two. These results lead him to conclude that in many cases, market transactions can generate privacy protections, but that there are also cases where markets may fail or transactions do not take place. What is needed, in his view, is a differentiated approach to privacy, which recognises that there is no single privacy solution. In some cases, markets would provide a solution, while in others, there would be a need for legislation or a stronger interpretation of constitutional safeguards.

From the foregoing discussion, it is fair to say that there would be numerous options as to how a structured market for personal information could be created. Much would depend on market forces and the active participation of both government and the private sector in giving shape to this market. Fundamental would be the creation of information property rights wherein information possessed commercial value.[52]

---

[51] Kenneth C. Laudon, Markets and Privacy, *Communications of the ACM*, September 1996/vol. 39, No.9.

[52] Whether the courts and the private sector would be agreeable to such a property right is not entirely clear. Eli M. Noam concludes that "Courts have been reluctant to grant property rights to personal information outside of the case of luminaries." See, "Privacy and Self-Regulation: Markets for Electronic Privacy," in *Privacy and Self-Regulation in the Information Age*, issued by the National Telecommunications and Information Administration, U.S. Department of Commerce, 1997. Kenneth C. Laudon concludes that "While there is much support for these ideas, surprisingly, market research, advertising executives, and others have raised objections to the notion that individuals should own their personal information..." *op.cit.*

Privacy-Enhancing Technologies (PETs) to Enhance Choice

Over the last few years, information technologies have appeared with the capability of enhancing instead of diminishing privacy protection (PETs). A technological solution to privacy seems a fitting approach in an age of information technology. That this capability has been recognized and increasingly utilized owes a great deal to the existing market demand for privacy protections. A technological solution may, therefore, be viewed as just another type of market solution. If hardware and software can be designed to incorporate privacy protections, and such technologies are readily accessible to the general public, PETs can become a core feature of how to resolve privacy problems raised by technology itself.[53]

The principal privacy-enhancing technology is strong encryption, which permits individuals to keep their communications and their identities confidential. In the context of our discussion of how markets could protect privacy, PETs can be viewed as a parallel approach. If the markets approach rests largely on property rights as providing the critical leverage for individuals to control their personal information, then PETs, through the use of various applications of encryption, could provide the technological leverage. Thus, an encrypted smart card could deny a company access to a customer's personal information during the execution of a transaction. The smart card would process the transaction without revealing any unnecessary identifying information – revealing only the minimum amount of personal information necessary to complete the transaction. E-cash technologies will also provide individuals with the ability to remain anonymous or near-anonymous. Further, the use of pseudonymous identifiers when surfing the Web or communicating online will strongly shield identifying information. By limiting access to personal information through the design of various emerging technologies, PETs will limit the creation of databases of personal information and the disclosure of that information to third parties.

To deal with the issue of how individuals can control the amount of personal information they reveal to a Web site they are browsing or with which they may wish to enter into a transaction, the World Wide Web Consortium (W3C) has sought to develop a method by which individuals can reveal their preferences about the degree of personal information they are willing to reveal. Called the Platform for Privacy Preferences or P3P, the standard would permit individuals to negotiate their privacy preferences with a particular Web site.[54]

---

[53] This and other themes are explored in Information and Privacy Commissioner/Ontario and Registratiekamer (Netherlands), *Privacy-Enhancing Technologies*, 2 vols., 1995.

[54] More information on P3P can be had from the World Wide Web Consortium <http://www.w3.org/P3P/>. AT&T Labs-Research is developing a P3P-based "Privacy Minder," a client-side proxy designed to be installed on a user's computer and work with the user's existing Web browser. Web sites will automatically communicate their privacy policies and users can configure browsers with their preferences. Microsoft and TRUSTe have introduced "Privacy Wizard," a free server-side digital tool kit for Web sites to easily create and post machine-readable privacy policies, which can be read automatically by a Web browser to determine whether a Web site's privacy practices are acceptable to a user.

One of the more sophisticated ways emerging to navigate the Web is through the use of 'intelligent agents,' or intelligent software programs[55] that may be programmed to each individual's specific interests or tastes, or in respect of one's privacy preferences. The agent could search, for example, Web sites that followed privacy practices that were in accordance with one's own preferences. While this technology is at the early stages of development for the more sophisticated agents, once some of the technical problems have been resolved, agents could become a useful way of ensuring the privacy of one's personal information on the Web. There are already indications that some businesses have seen the potential for using intelligent agents to serve the needs of both the company and customers, by selling the personal information they possess and compensating the consumer for the use of that information.[56] A word of caution, however — intelligent agents can either become a friend or foe of privacy, depending on their design and the manner in which they are programmed to operate.[57]

A new approach that appears to be gaining momentum is that of the "infomediary," or information intermediary.[58] This approach recognizes the economic and strategic value of consumer information on the Net for both business *and* consumers, and builds on that premise. Customers are beginning to realize that vast amounts of identifiable information are being collected about them without their consent, as they use various online services. This information, including their clickstream, surfing and purchasing habits, is vital for companies seeking to develop and sustain specific market relationships. Such consumer profiles greatly enhance vendors' ability to focus their marketing efforts.

As the collection of personally identifiable information by online services has grown, so too has public concern about online privacy. In an effort not to alienate their online customers, companies are beginning to become mindful of consumer privacy. And yet, the cost of "permission marketing," which requires customer consent prior to initiating marketing efforts, can be significant. As noted earlier in the discussion on the nature of the existing market for privacy, from the consumers' perspective, it is extremely time consuming and difficult to negotiate, one-on-one, with each organization in an attempt to reach an agreement with regard to protecting their personal information. This difficulty is perhaps even more pronounced in the online world where business transactions take place remotely and across multiple jurisdictions.

---

[55] For more information on intelligent software agents, see the Web site of the University of Maryland Baltimore County's Laboratory for Advanced Technology <http://www.cs.umbc.edu/lait/>. See also the work of the Agents Research Programme, BT Laboratories' Intelligent Systems Research (ISR) Group. <http://www.labs.bt.com/projects/agents/>

[56] Patrick Brethour, "New breed of data dealer woos consumer," *The Globe and Mail*, April 1,1998.

[57] Information and Privacy Commissioner/Ontario and Registratiekamer, The Netherlands, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector*, May 1999.

[58] The concept of "infomediaries" was developed and examined by John Hagel III and Marc Singer in their book, *Net Worth: Shaping Markets When Customers Make the Rules*, Harvard Business School Press, 1999.

An infomediary would act as a personal agent or trusted third party who would negotiate with online services on behalf of their consumers. One commercial infomediary defined the term as "a trusted third party, one who connects information supply with information demand and helps to determine the value of that information."[59] Another described its service as: "Providing individuals with the power to profit from their personal profiles.... Providing corporations with the power to profit from personalization."[60]

In theory, consumers would provide an infomediary with their personal information as well as instructions on if, how, and when their information could be disclosed. The infomediary would then become the custodian of that information, providing businesses with limited access to it under the conditions set by the individual. The information could be in aggregate or identifiable form, depending on the terms set by the consumer. By removing direct contact with individuals, and introducing a layer between them and online vendors, this model should enhance consumer privacy. The idea is to enhance the benefits to consumers by giving them personal choice, and if desired, compensation for controlled access to their personal information, while shielding their identity from unwelcome vendors. This approach builds on the structured market model which necessitates a recognition and compensation for the commercial value of personal information. It also offers the potential for anonymous transactions.

The issuance of trusted seals to Web sites that conform to certain privacy principles is more of an administrative solution to the problem. TRUSTe has become the leader in this approach, licensing its TRUSTe seal to appear on Web sites that maintain prescribed privacy practices, which are also subject to audit by independent assessors. The Better Business Bureau has developed a similar privacy seal through its BBB Online program. Another example of a privacy seal offered by a trusted association is WebTrust, developed by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants. It may well be the case that such approaches, as exemplified by various trustmarks, will work well in a Web-based environment. The public has come to understand the meaning of such trustmarks in different commercial contexts, and may thus be able to transfer that experience to the electronic environment.

A final category of PETs involve the use of digital pseudonyms. This is a method of identifying an individual online through an alternate digital or pseudo-identity, created for a particular purpose. It permits users to preserve their anonymity by concealing their true identities behind pseudonyms. Users are only known in various online contexts by their "nyms," for the purpose of participating in selected activities (such as chatting in a newsgroup or subscribing to a listserv). While a number of promising anonymizing technologies have

[59] PrivaSeek at <http://www.privaseek.com>

[60] Infomediary at <http://verion.com>

recently appeared on the horizon, we believe one deserves special mention.[61] "Freedom" by Zero Knowledge Systems offers true anonymity in that no one, not even the systems operators, will have any knowledge as to the identity of the those who subscribe to the service.

By restoring the anonymous option to online transactions, this type of technology could empower the consumer to obtain a desired product or service without disclosing his or her personal information. It can provide a positive exception to the statement noted earlier that for most business transactions, an individual cannot choose to receive goods and services without providing some personal information. Although still in the early stages, it offers the potential to establish another model within the commercial framework that recognizes privacy, not as a hindrance, but as a social value that can be protected, while still not interfering with the market.

[61] At the time of publication, a number of anonymizing or pseudonymous schemes had been announced, including: Anonymizer <http://www.anonymizer.com/3.0/index.shtml>; Lucent Technologies' ProxyMate <http://www.proxymate.com>; and Zero-Knowledge's Freedom <http://www.zeroknowledge.com>. On April 7, 1999, Zero-Knowledge released a paper discussing pseudonoymous communication in the context of provisions of the European Union's Data Protection Directive. The paper, entitled *EU and the US: The Efficacy of Data Protection Legislation and the Anonymous Solution*, is located at <http://www.zeroknowledge.com/policy>. Other anonymizing technologies under development are: AT&T Labs-Research and Bell Labs' "Crowds." This system simulates a "virtual" crowd to obscure an individual's Web activity by randomly routing user information requests to inhibit tracing the request to any one user; "Onion" is similar type of anonymous routing system, developed by the Naval Research Laboratory. This system bounces messages through a series of routers in a random order on the way to their destination.

Conclusion

There is every indication that privacy will remain a continuing challenge well into the 21st century. What today may look like a patchwork of privacy protections could, in the next century, encompass a privacy architecture that provides different solutions for different contexts. What that final architecture will be is not entirely clear, though the outlines of a privacy architecture are discernible.

This paper has sought to explore the practical implications for individual control and personal choice that are raised by the different perspectives canvassed. In the process, some interesting insights have presented themselves.

The economic perspective argues that individuals in large institutional settings are likely to be disadvantaged in their ability to exercise control and exert personal choice over how their information will be used. Individuals are said to have asymmetrical information and bargaining power relative to various organizations. Under these conditions, individuals are not in an ideal position to exercise control or make informed choices with respect to the uses of their personal information. The policy issue in these circumstances is how to redress the balance so that individuals can find themselves in a better position to exercise such control.

In dealing with asymmetrical information, individuals need to have available sufficient information about institutional behaviour and information practices to be able to make an informed choice as to whether or not to enter into transactions with an organization. Several approaches could be used to inform individuals of these issues. Organizations could undertake to provide sufficient information on their privacy policies to enable individuals to make informed decisions. Ethical considerations and competitive pressures could create the motivation for businesses to post their privacy policies. However, resorting to legislation can be compelling if a sufficient number of organizations do not adopt such an approach (the existing status quo).

Dealing with asymmetrical bargaining power, individuals require mechanisms that will enforce their personal choices. In the public sector, given the coercive power of the state, legislated privacy rules and fair information practices can provide some balance to the individual's asymmetrical bargaining power. In the private sector, meaningful self-regulation is also an option. Theoretically, a market-based approach could work if property rights were assigned to personal information, permitting individuals to exercise control over their information, thus allowing them freedom of choice over its collection, use and disclosure. However, in order for the market-based approach to work properly, a structured market needs to be in place.

One might argue however, that privacy, when viewed as a fundamental human right, cannot simply be bought and sold — it should not be traded away to the highest bidder. While this may ring true, does it necessarily apply to every situation? Our view is that in the context of

the rights of citizens in relation to the state, privacy should not be put on the table for negotiation. To do so would threaten any legislated protections already in place. As Professor Noam noted:

> ...a distribution of privacy rights on a free-market basis would provide no protection for citizens against encroachment by the state. The only effective limits on government are those established through constitutional means. Therefore, any system which allocates privacy according to the open market would also need constitutional provisions barring infringements by the state.[62]

We agree. Legislated protections must continue to safeguard fundamental human rights relating to the state, with restrictions placed on the uses of our information by government. Accordingly, the first element of the privacy architecture would include data protection as embodied in fair information practices, and implemented through legislation or effective self-regulation covering the public and private sectors.[63] Data protection can be viewed as a way to deal with informational privacy in the context of record keeping practices, where personal information is collected, stored and used for administrative and operational purposes. It provides a baseline protection, particularly in terms of restricting secondary use, provide data subject access and ensures a mechanism for enforcement. Fair information practices establish a pro-privacy method of operation, a position of strength, from which individuals can choose to negotiate exceptions as they wish.

Any consideration of market-based protections should only be made in the private sector, in the context of commercial transactions. Information property rights could be another element in the privacy architecture. If one possessed property rights over one's personal information, individuals could exercise the control they presently lack. From the individual's perspective, such a property right could provide a practical way of addressing the problem of unauthorized disclosure of one's information to third parties, or the secondary market for personal information, which, in our view, represents one of the most serious threats to privacy, subject to the greatest abuse. With respect to the *commercial* uses of one's personal information, an information property right that would ensconce the right to control one's property (in this case, one's information), may have some merit.

While the notion of owning one's personal information, information as property, may be appealing in a commercial context, it is not without its critics. Some argue that this would burden the poor disproportionately. Perhaps it would. But while this may be true, who would decide? Who should be making these decisions? Surely not the privileged, acting on behalf of the poor, presuming to know what is in their best interests. As Noam points out,

---

[62] Eli M. Noam, *Privacy in Telecommunications: Markets, Rights and Regulations*, manuscript, 1993.

[63] It must be noted that the IPC has actively lobbied for the introduction and adoption of Bill C-54 to regulate data protection in Canada's private sector. As the provincial oversight agency responsible for the protection of privacy in Ontario, we support the federal government's commitment to enact legislation establishing a set of data protection principles for the private sector. See the IPC's remarks to the Standing Committee on Industry, December 3, 1998 and February 17, 1999.

> ... a poor person's priorities may often not include privacy protection. ... The poor are best helped by more money; to micromanage their condition through restricting their right to transact may well end up a patronizing social policy and an inefficient economic policy.[64]

The present-day reality is one in which the personal information of the public — both the rich and the poor — is being freely used for commercial purposes, without seemingly any direct or obvious financial remuneration or benefit to the individual. Obtaining economic benefits for the permitted uses of one's personal information may be an idea worth exploring. If consumers were presented with market-based options for the commercial uses of their personal information, we believe that considerable interest would be shown.[65] This, in addition to legislation protecting our fundamental human rights, and, at a minimum, protecting privacy from intrusions from the state, may present a comprehensive model. Privacy protection need not be presented as an either/or proposition — *either* as a fundamental right *or* as an economic interest. To varying degrees, it can be both, if that represents an individual's wishes. The final choice must always lie with the individual.

Privacy-enhancing technologies or PETs are another element in this privacy architecture, offering potential privacy solutions in the context of electronic communications that identify individuals during interactive sessions. PETs could restrict the gathering of personally identifying information through a variety of means building on encryption, during the course

---

[64] Eli M. Noam, *Privacy in Telecommunications: Markets, Rights and Regulations*, manuscript, 1993.

[65] A 1999 survey on information-for benefits programs conducted by Privacy & American Business and Opinion Research Corporation (*"Freebies" and Privacy: What Net Users Think*) noted that "an overwhelming majority of Net users [86%] believe collecting information on their buying habits and preferences to tailor offers and services is fair, and participating in these programs should be a matter of individual privacy choice." <http://www.pandab.org/pr990714.html>

An example of consumers choosing to disclose their personal information in exchange for a perceived economic benefit occurred in February 1999 when two companies offered free computers to consumers who agreed to certain conditions.

Free-PC.com announced it would give personal computers to the first 10,000 people to provide access to their consumer information, including age, income, family status, hobbies, and buying habits. Once they got their computers and turned them on, recipients received advertisements. The company planned to monitor how the computer was used, track which of its ads were clicked on as well as where users went, and what they bought on the Web. Reportedly Free-PC.com received 375,000 applications on the first day. <http://www.wired.com/news/print_version/email/explode-infobeat/business/story/17783.html?wnpg=all>

Two days after Free-PC made its announcement, One Stop Communication offered 25,000 free iMacs. Two hours after that deal was announced 2,500 people had signed up. While the Free-PC scheme was to give computers to users willing to disclose personal information and receive ads, One Stop Communication was to give an iMac to anyone promising to spend US$100 a month at its online mall for the next three years. Users also had to commit to using One Stop Communication as their Internet Service Provider. Customers were to provide One Stop with their credit card number or enough personal information to prove their credit-worthiness. According to the deal, each month, a shopper was to spend at least US$25 at an online mall. If a shopper did not shop, his or her account was charged US$100. Reportedly, the consumer commitment represented a US$3,600 outlay for a computer valued at US$999. <http://www.wired.com/news/news/business/story/17863.html>

of such sessions. These technologies offer another way for individuals to exercise freedom of choice, by permitting them to engage in transactions without revealing personal information unnecessarily, or without revealing any identifying information at all. Emerging technologies, especially those focussing on anonymous and pseudonymous identifiers, may well advance as the primary means of protecting online privacy.

The different perspectives discussed in this paper suggest that the protection of personal information will likely only be possible through the application of a variety of techniques. Consumer groups, privacy advocates and data protection commissioners can provide information on how organizations should collect, use and disclose personal information in accordance with fair information practices. We can also educate the public on the existence of different privacy-enhancing technologies, as well as monitoring their development. For privacy advocates, the prevailing issue is to assist the public in understanding the different approaches to privacy protection and to contribute to finding effective solutions that can truly enhance people's ability to exercise control.

This paper has identified the structural elements of a comprehensive privacy architecture, one which could provide appropriate levels of control and choice for individuals, depending on the context in which they entered into different institutional relationships with government or private sector organizations. Some convergence has emerged with respect to various elements of the architecture. It is generally agreed upon that fair information practices constitute the foundational structure of privacy protection, whether they are realized through legislation, or through self-regulation. Privacy-enhancing technologies also represent a structural element in that architecture. What remains unclear is whether a structured market for personal information based on property rights will ever form a structural element in the privacy architecture of the future.

We believe that creating a privacy architecture for the 21st century is both feasible and desirable — one which extends to both private and public sectors and which incorporates the elements described above. For our part, we will endeavour to fulfill the public responsibilities of our agency by contributing to the debate on these different approaches and working to inform the public as to the multitude of choices available in protecting one's privacy.